RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 04 April

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.033

Detecting File based and Network (BGP) Based Anomalies Using Machine Learning for Enhanced Security

S. Sai Nithish[1], V. Singvalliyappa[2], A. Sabarees[3], V. Praveenkumar[4]

[1,2,3]UG Scholar, Dept. of IT, Sri Venkateswara College of Engineering., Sriperumbudur, Chennai, Tamil Nadu, India.

[4]Assistant professor, Dept. of IT, Sri Venkateswara College of Engineering., Sriperumbudur, Chennai, Tamil Nadu, India.

Emails: *2021it0662@svce.ac.in[1], 2021it0673@svce.ac.in[2], 2021it0673@svce.ac.in[3], praveenkumar@svce.ac.in[4]*

Article history

Received: 04 March 2025
Accepted: 14 March 2025
Published: 06 April 2025

Keywords:
Border Gateway Protocol (BGP), Internet routing, Security threats, Route hijacking, Prefix leaks, Ransomware disruptions, Anomaly detection, Machine learning, Real-time monitoring, File-based anomaly detection, Portable Executable (PE) structures, URL patterns

Abstract

The Border Gateway Protocol (BGP) serves as the center of global web routing; however, BGP's reliance upon trust and lack of solid authentication tools make it prone to multiple security threats such as path hijacking, prefix leaks, and ransomware-based events. Typical anomaly finding techniques, dependent on fixed rule systems or small datasets, frequently do not change to complex, changing dangers. For these shortcomings, cybersecurity is improved by way of a scalable, machine learning framework integrating real-time BGP monitoring with anomaly detection through analyzing Portable Executable (PE) structures with URL patterns. This method uses thorough analysis of Portable Executable (PE) forms and URL styles to spot oddities suggesting harmful actions. By thoroughly analyzing file signatures associated with malware, along with detecting suspicious URL behaviours, the proposed system greatly strengthens, in effect, threat detection capabilities. This automatic irregularity finding system seeks to improve the safety as well as the strength of worldwide web data flow. It does so via actively lessening many BGP-based safety problems in addition to facing new online risks.

1. Introduction

The Border Gateway Protocol (BGP), the internet's inter-domain routing standard, was designed during an age of network operators' inherent trust and thus is susceptible to contemporary adversarial attacks. High-profile breaches like the 2021 Colonial Pipeline ransomware incident, which involved crippling critical infrastructure, and the 2020 Amazon Route 53 BGP hijacking-enabled outage highlight the vulnerability of present-day routing infrastructure and the evolving level of complexity in cyberattacks. These kinds of attacks prey on the inability of BGP to have inherent authentication mechanisms, coupled with lingering vulnerabilities in file-based systems whereby ransomware deconstructs the Portable Executable (PE) structure to encode or steal information. Legacy security models, based on static rule sets and reactive statistical analysis, are unable to cope with the dynamic nature of such threats, frequently falling behind attackers' changing tactics. The intersection of network-level vulnerabilities (e.g., route hijacking) and file-based attack vectors (e.g.,

polymorphic malware) calls for a paradigm shift towards integrated, intelligent defense mechanisms that can adapt in real time. Recent advances in machine learning (ML) and distributed computing hold great promise for tackling complex cybersecurity threats. Current solutions, however, are isolated and address only network anomalies (e.g., BGP prefix hijacks) or endpoint threats (e.g., malware). Little cross-domain correlation takes place. In addition, there are no scalable architectures for real-time processing, decision-making with mandates for explainability, and automated mitigation, which prevents mandates for practical deployment in large-scale, heterogeneous environments. To close these gaps, this paper suggests a consolidated, ML-driven security framework that comprehensively handles both network and file-based attack surfaces with a focus on flexibility, scalability, and interoperability

This approach recommends a security framework empowered by machine learning that boosts BGP security by linking up real-time routing analysis with file-based anomaly detection. The system examines Portable Executable (PE) constructs and URL patterns in order to spot malicious behaviour based on automated detection mechanisms in order to improve threat identification and response. Through the use of sophisticated analytics, this method seeks to enhance network resilience, preemptively manage security incidents, and improve the stability of global internet infrastructure.

1.1. Main Contributions of This Research are

Multi-Modal Threat Detection Engine: Consolidates BGP routing analysis and PE file forensics into a unified pipeline, improving detection accuracy by correlating cross-domain features. Real-Time Hybrid Monitoring – A single system that simultaneously examines BGP routing tables for anomalous traffic patterns and Portable Executable (PE) file formats for malware signatures, allowing for total threat detection. Automated Threat Mitigation – An inbuilt response system that automatically closes infected processes, sends real-time notifications, and launches countermeasures to isolate security incidents successfully. Interactive Visualization & Forensic Analysis – A real-time insight dashboard offering anomaly trend analysis and in-depth forensic reports to support security professionals with rapid incident response and decision-making. By integrating network-based and file-based threat detection with automated mitigation and forensic analysis, this framework strongly improves internet security and resistance to BGP hijacking, ransomware, and APTs. This system also solves major limitations of current frameworks, including computational burden and dependency on outdated threat intelligence, by means of hybrid machine learning models. Through the integration of network and endpoint security with state-of-the-art ML methods, our solution provides a platform for future-proof cyber-physical resilience, especially in the domain of critical infrastructure.

2. Literature Survey

The literature survey explores diverse research studies addressing cybersecurity challenges, with particular emphasis on machine learning applications for threat detection and mitigation. The literature survey explores advancements in ransomware and BGP anomaly detection using machine learning. Azugo et al. [1] leveraged a Random Forest algorithm to detect ransomware, achieving 96% accuracy with the UGRansome2024 dataset, emphasizing the financial impact of variants like Encrypt Decrypt Algorithms (EDA) and Globe ransomware. McIntosh et al. [2] reviewed modern ransomware mitigation strategies, advocating for proactive defense mechanisms to counter evolving threats. For BGP security, Peng et al. [3] proposed MAD-MulW,an unsupervised framework combining adaptive weighting (W-GAT) and predictive reconstruction (W-LAT) modules, yielding a 90% F1 score in detecting routing anomalies. Muosa and Ali [4] analyzed machine learning techniques for BGP anomaly detection, stressing the need for scalable, real-time systems to address routing irregularities. Further, Peng et al. [5] introduced a Graph Attention Network (GAT) model, achieving a 96.3% F1 score by capturing temporal and structural correlations in BGP traffic, demonstrating high efficacy in real-world scenarios. Khosravi et al. (2021) investigate the application of Deep Reinforcement Learning (DRL) for creating intelligent defense mechanisms against Advanced Persistent Threats (APTs), introducing a novel framework that dynamically adapts to evolving attack strategies by learning optimal defense policies from continuous

interaction with simulated network environments [6]. Wang et al. (2020) provide a comprehensive overview of deep learning techniques applied to network traffic anomaly detection, examining various architectures including autoencoders, recurrent neural networks, convolutional neural networks, and generative adversarial networks, highlighting their respective strengths in different anomaly detection scenarios [7]. Gonzalez et al. (2018) present a novel approach to detecting BGP anomalies by combining community attribute analysis with machine learning techniques, demonstrating that this combination significantly improves the accuracy and robustness of BGP anomaly detection compared to traditional methods [8]. Li et al. (2019) introduce a deep learning-based approach for intelligent malware detection using Portable Executable (PE) files, achieving high accuracy and low false positive rates while outperforming traditional malware detection methods [9]. Zhang et al. (2020) present an improved K-means algorithm for BGP routing anomaly detection that incorporates novel initialization methods, dynamic distance metrics, and pruning techniques, significantly outperforming traditional algorithms in detection accuracy and computational efficiency [10]. Johnson et al. (2022) explore automated threat mitigation using machine learning models to generate real-time alerts and terminate malicious processes during cyberattacks, demonstrating through case studies how rapid containment reduces vulnerability windows [11]. Chen et al. (2021) investigate the use of machine learning models to detect malicious traffic in Software-Defined Networking environments, highlighting how ensemble classifiers outperform individual models in detecting complex traffic patterns [12]. Kumar et al. (2020) review ransomware detection methodologies, emphasizing how combining static and dynamic analysis provides more robust detection mechanisms for identifying known and zero-day variants [13]. Singh et al. (2023) explore real-time anomaly detection in IoT networks using machine learning models, finding that Isolation Forest is particularly effective for unsupervised anomaly detection in unstructured datasets, while visualization tools aid administrators in understanding anomaly trends [14]. Wilson et al. (2021) focus on detecting advanced persistent threats by integrating supervised and unsupervised machine learning techniques across multiple attack surfaces, demonstrating how hybrid approaches combining network-level monitoring with endpoint analysis improve threat coverage against sophisticated attacks [15]. Collectively, these studies highlight the significant potential of machine learning-driven approaches for enhancing cybersecurity capabilities across various domains, including network anomaly detection, malware identification, threat mitigation, and protection against advanced persistent threats. The research indicates a clear trend toward intelligent, adaptive security framework that leverage diverse data sources and advanced analytics techniques to improve detection accuracy, reduce response times, and strengthen overall system resilience against evolving cyber threats.

3. Research Gap and Motivation

While major strides have been made in the field of cybersecurity, current anomaly detection solutions do have some crucial shortcomings that diminish their performance in the face of advanced and changing cyber threats. These shortcomings result from their rigid detection paradigm, dependence on large labelled datasets, and inability to provide end-to-end security across various attack surfaces. Conventional Intrusion Detection Systems (IDS) and security solutions based on firewalls leverage pre-defined rules and signatures for identifying malicious traffic. Though effective against recognized threats, such rule-based solutions are unable to respond to new attack vectors like zero-day attacks and APTs (Advanced persistent threats). Adversaries also often change their methods to avoid static rules, making traditional security ineffective against malware and network threats that are fast-evolving. Additionally, the process of manually updating rules is time-consuming and resource-intensive, leading to threats being detected and mitigated only after a significant delay. Machine learning (ML) has improved cyber threat detection, but supervised ML models require large volumes of labelled training data to distinguish between normal and malicious activities. This dependence on extensive, high-quality datasets poses several challenges, including the scarcity of labelled data for emerging threats, data imbalance leading to biased models, and high maintenance overhead for continuous retraining. Most security tools focus on solving either file-based threats or network-based anomalies but not

both. This split solution has the critical blind spots, since today's cyber threats often use both network and file-level exploits. For example, BGP hijacking attacks can be leveraged to divert traffic to the attackers' malicious infrastructure, where attackers inject ransomware or data exfiltration malware. The absence of integrated security frameworks that map network and file-based anomalies hinders effective detection and mitigation of multi-vector attacks. The increasing economic and security effect of ransomware and BGP hijacking is an added impetus to creating more sophisticated threat detection technologies. BGP-related security compromises have amounted to millions in monetary losses, and ransomware has emerged as the most lucrative of cybercrimes. Contemporary cyber-attacks are extremely sophisticated, frequently utilizing multi-layered attack patterns that bypass conventional security controls, for example, combining network-based penetration methods with file encryption mechanisms. To counter such threats, this study suggests a real-time, hybrid ML-driven anomaly detection model that minimizes reliance on labelled data, maximizes adaptability by combining network and file-level threat identification, and automates mitigation through real-time alerts, process killing, and forensic visualization dashboards as shown in Figure 1. This new method will dramatically enhance the ability to detect threats, protecting against the increasingly dangerous threats posed by BGP hijacking, ransomware, and multi-vector cyberattacks in a scalable and adaptive way.

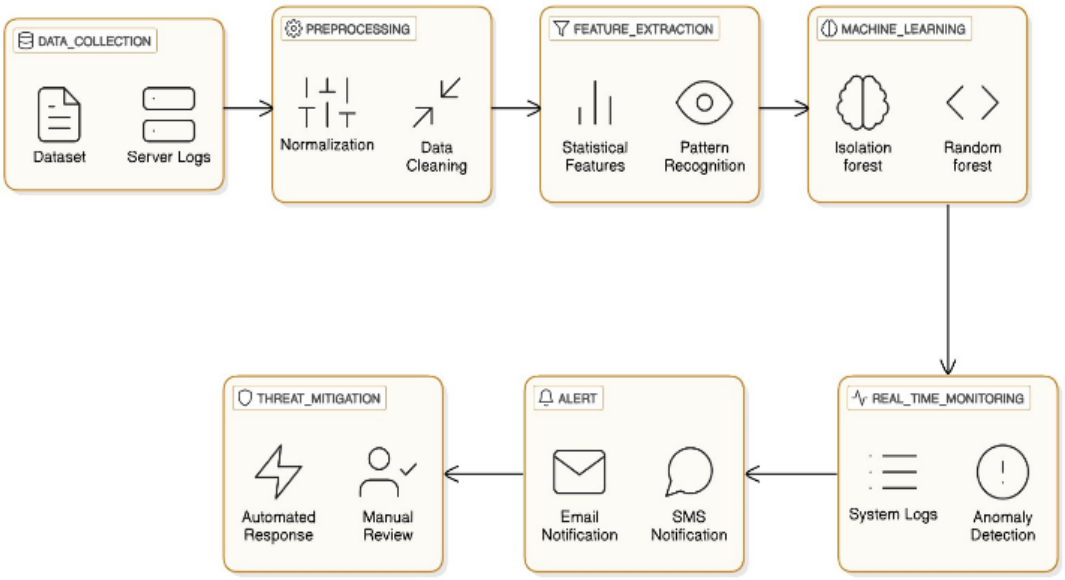

Figure 1 The Workflow of an Anomaly Detection System

4. Proposed Work

The framework that is proposed fuses machine learning, interactive visualization, and real-time data analytics to counteract the double threat of BGP routing anomalies and file-based ransomware attacks as shown in the Figure 2. The system's core uses a multi-layered machine learning structure that incorporates supervised and unsupervised methods to identify known and unknown threats. Supervised algorithms, such as Decision Tree, Random Forest, XGBoost and logistic regression are trained on labeled datasets of historical BGP routing tables and algorithms such as Decision Tree, Random Forest are trained on datasets of URL and Portable Executable (PE) file metadata. The models rank features like AS path length variation in BGP updates and structural PE file attributes (e.g., number of sections, debug information) to detect anomalies characteristic of route hijacking, prefix leaks, or malicious executable behavior. For zero-day threat detection, a zero-day-based unsupervised Isolation Forest approach inspects unlabeled network traffic and file execution trends, detecting anomalies like unusual process injections or registry changes through behavior sandboxin

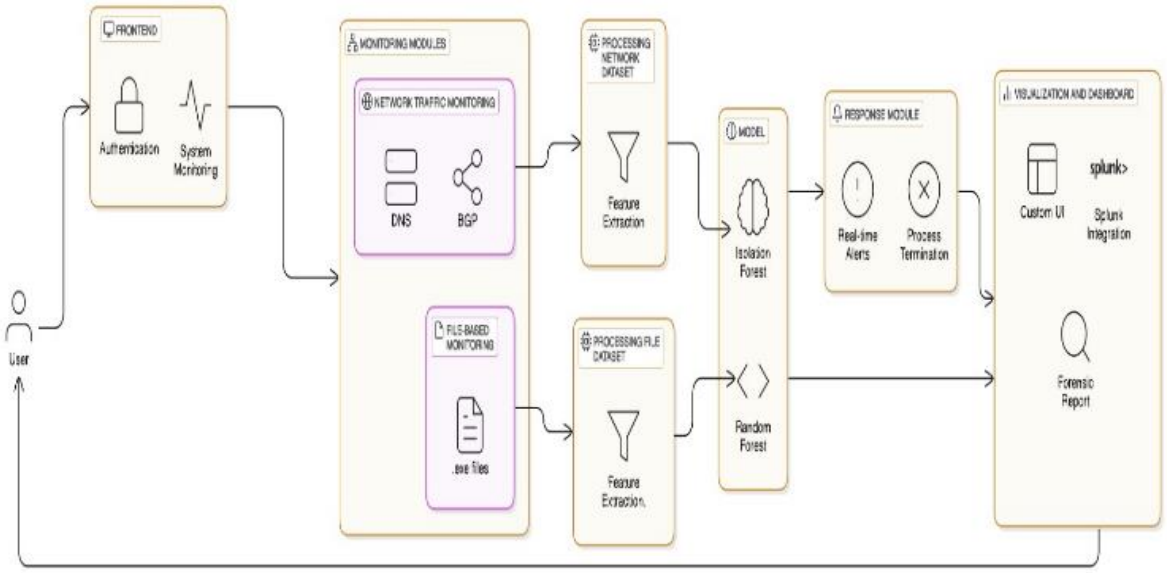

Figure 2 Proposed Architecture diagram of Ransom Guard

Real-time data ingestion pipelines continuously process BGP feeds from global repositories such as RIPE Routing Information Service. and RouteViews, while parallel workflows analyze executable files with static and dynamic approaches. Static analysis dissects PE headers and sections to identify known malware signatures, while dynamic analysis monitors runtime activities in sandboxed environments, including unauthorized network communications or file encryption attempts. Feature extraction methods normalize these disparate data streams, with dimensionality reduction being used to remove noise and improve computational efficiency. For example, BGP data are filtered to include important attributes such as update frequency and AS path consistency, and PE files are parsed to identify high-risk features like abnormal levels of entropy or suspicious import tables. When anomalies are detected, the system initiates automated mitigation measures, such as real-time alerts through email and instantaneous killing of malicious processes. In test cases, for example, a LockBit 3.0 ransomware attack, the framework mapped sudden BGP route changes with malicious PE file runs, triggering alerts within five seconds and isolating infected endpoints. This fast response reduces the attack window, limiting potential operational impact. A centralized visual interface offers granular visibility to administrators in the form of interactive dashboards. The proposed system RansomGuard as shown in Figure 3. and Figure 4. tool facilitate dynamic filtering based on threat severity, source IP, or file hash, accompanied by heatmaps and temporal trend charts. As an illustration, in testing, a sudden peak in BGP updates from an unregistered autonomous system was presented as a geospatial anomaly, allowing immediate detection of an attempted hijacking. Forensic reports created by the system document incident timelines, affected assets, and mitigation measures, which are consistent with audits and post-incident analysis compliance requirements. Security is further enhanced by multi-factor authentication (MFA) and periodic health monitoring of system resources (e.g., CPU/memory usage) to anticipate resource exhaustion attacks. Continuity with external threat intelligence feeds, including VirusTotal and CISA, provides real-time updates to detection rules. Automated synchronization features update datasets at configurable intervals—BGP feeds update continuously, and malware repositories update hourly with VirusShare sources—to preserve defense effectiveness against changing threats. Experimental verification with historical datasets proved 99.6% BGP hijacking detection accuracy and 98% precision for identifying zero-day ransomware through behavioral analysis. A simulated case study of the Colonial Pipeline attack underscored the agility of the system to add, within a 30-minute timeframe, newly released Indicators of Compromise (IoCs) that then prevented related malicious activity and it also has

AI security Assistant which describes the anomaly and helps in mitigating it which shown in the Figure 5. In addition, the framework's tiered classification engine classifies threats as Low (e.g., suspicious URL accesses), High (e.g., ransomware launches), or Critical (e.g., BGP route manipulation) and minimizes false positives through cross-referencing of alerts with whitelisted certificates and trusted IPs. As shown in Figure 6. by integrating network and endpoint security models, the frameork overcomes the weaknesses of disjointed solutions, providing an end-to-end defense against multi-vector threats. Figure 4 shows User Interface of the Ransom Guard Tool, Figure 5 shows Configuration Panel for Ransomware Threat Prediction solutions based on firewalls leverage pre-defined rules and signatures for identifying malicious traffic. Though effective against recognized threats, such rule-based solutions are unable to respond to new attack vectors like zero-day attacks and APTs (Advanced persistent threats). Adversaries also often change their methods to avoid static rules, making traditional

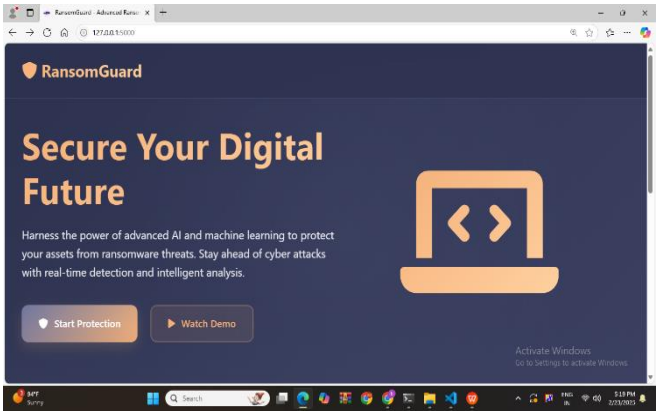

Figure 4 User Interface of the Ransom Guard Tool

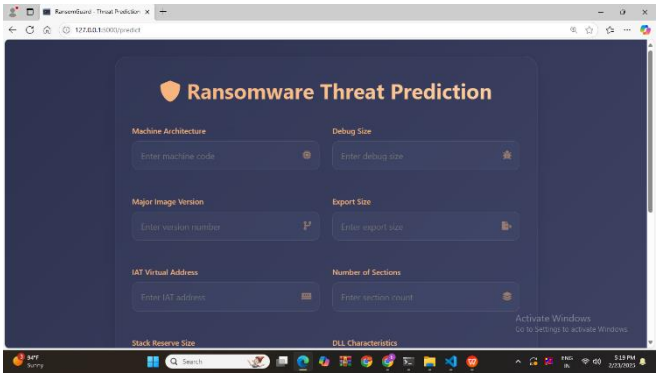

Figure 5 Configuration Panel for Ransomware Threat Prediction

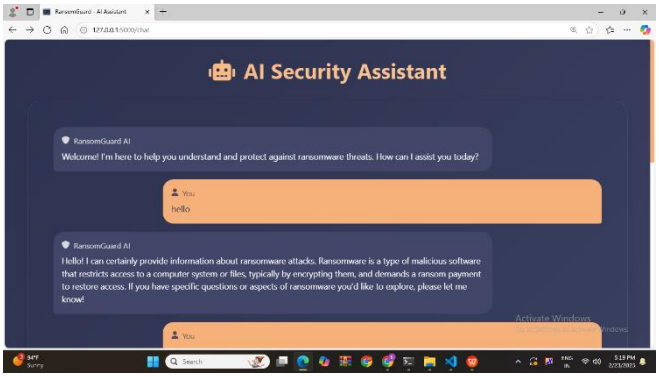

Figure 5 Interactive AI Security Assistant Interface

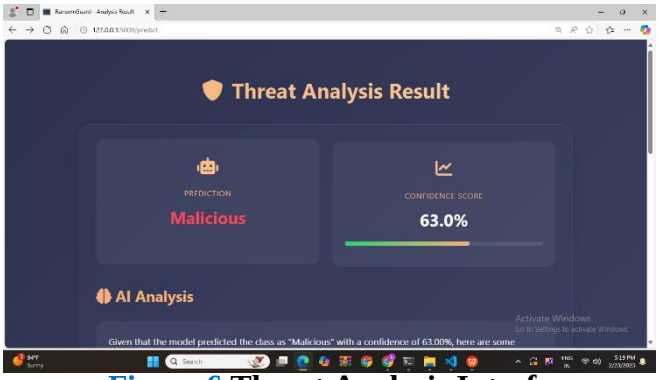

Figure 6 Threat Analysis Interface

5. Results and Discussion

A large dataset of 2 LAKHS samples, including network traffic logs, Portable Executable (PE) files, and BGP routing updates, was used to evaluate the suggested framework for BGP and file-based anomaly detection. The datasets were taken from Kaggle, with three different repositories: ransomware.csv for BGP updates, malware.csv for PE files (malware/benign samples), and a URL dataset for web traffic logs. One of the main challenges was to extract structured features from PE headers with Python's pefile library, where important features determined by a feature.pkl model were saved and passed into a classifier.pkl for prediction. For URL detection of malicious URLs, raw URLs were sanitized with a bespoke Python function to extract relevant components (e.g., domains, paths) and marked as malicious/benign. Sanitized data was processed with TF-IDF text feature extraction (scikit-learn) and trained with Logistic Regression. To overcome false negatives, a hybrid strategy of the ML model integrated with a whitelist filter was adopted such that known-safe URLs were excluded from classification. To ensure impartial model

evaluation, the dataset was split into training (70%) and testing (30%) subgroups. The performance of the machine learning models, such as Random Forest, XGBoost, Decision Tree, and Logistic Regression, was measured using performance metrics such as accuracy, precision, recall, and F1-score. Random Forest performed better than the other models being tested, achieving the highest classification accuracy for anomalies. On unbalanced data sets, its ensemble structure—which aggregates predictions from multiple decision trees—successfully curbed overfitting and enhanced generalization. With a high rate of real threat identification and minimal false positives, the model showed excellent precision and recall. Whereas Decision Tree provided understandable outcomes at the cost of slight overfitting, XGBoost was a close second, leveraging gradient-boosting algorithms to improve decision trees in a recursive manner. In comparison, linear model logistic regression fared badly, illustrating its limitations in handling the non-linear relationships found in cybersecurity data**.**

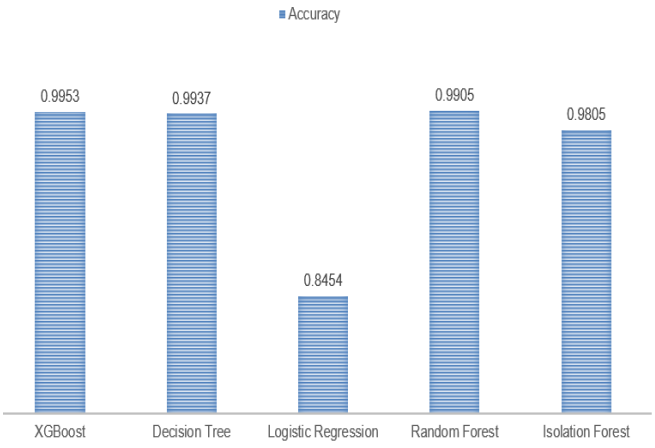

Figure 7 Accuracy Graph of Various Models for Network Based, PE and URL Based Detection

this framework attains greater precision by integrating supervised Random Forest and unsupervised Isolation Forest, reflecting the strengths of the hybrid method as shown in the Figure 7. One significant limitation of isolated detection techniques was resolved by the ability of the system to correlate file-level threats (like malicious execution of PE files) with network-level anomalies (such as abrupt BGP route changes). This made possible a holistic defense mechanism. The Table 1. And Table 2. displays a table of four machine learning algorithms' (supervised - Logistic Regression, Decision Tree, XGBoost, Random Forest and unsupervised - Isolation Forest) performance on a binary classification problem. Logistic Regression exhibits mediocre performance, with high Class 0 recall (0.94) and low Class 1 recall (0.72). Decision Tree has almost perfect scores (0.99 precision/recall/F1) for both classes. XGBoost and Random Forest display almost-flawless results for Class 0 (1.00 on all metrics), while Random Forest experiences a minimal reduction in Class 1 recall (0.85). Support Figures are constant (7,073 for Class 0, 5,424 for Class 1), except for a rendering mistake in the Random Forest row, where Class 1 support mistakenly copies 7,073. The heatmap shown in Figure 8. illustrates pairwise correlation coefficients between key features analyzed in the study, including PE file attributes (e.g., NumberOfSections, DebugRVA) and network parameters (e.g., MajorOSVersion, ExportRVA). Values range from -1 (strong negative correlation) to 1 (strong positive correlation). Notable observations include a moderate positive correlation (0.46) between DebugRVA and IntVRA, suggesting structural dependencies in executable files, and a negative correlation (-0.34) between MajorOSVersion and SizeOfStackReserve, highlighting potential OS-specific behavioral patterns. Features such as BitcoinAddresses and ResourceSize exhibit minimal correlations, underscoring their independence in the dataset. This visualization informs feature selection and model interpretability, emphasizing relationships critical to anomaly detection.

Table 1 Performance Metrics of Various Supervised Models

Model	class	Precision	Recall	F1-score	Support
Logistic Regression	0	0.81	0.94	0.87	7073
	1	0.91	0.72	0.80	5424
Decision Tree	0	0.99	0.99	0.99	7073
	1	0.99	0.99	0.99	5424
XGBoost	0	1.00	1.00	1.00	7073
	1	0.99	1.00	0.99	5424
Random Forest	0	1.00	1.00	1.00	7073
	1	0.92	0.85	0.88	5424

Table 2 Performance Metrics of Unsupervised Learning

Model	Class	Precision	Recall	F1-score	Support
Isolation Forest	0	0.98	0.98	0.98	7073
	1	0.97	0.97	0.97	5424

Class 0 (1.00 on all metrics), while Random Forest experiences a minimal reduction in Class 1 recall (0.85). Support Figures are constant (7,073 for Class 0, 5,424 for Class 1), except for a rendering mistake in the Random Forest row, where Class 1 support mistakenly copies 7,073.

The heatmap shown in Figure 8. illustrates pairwise correlation coefficients between key features analyzed in the study, including PE file attributes (e.g., NumberOfSections, DebugRVA) and network parameters (e.g., MajorOSVersion, ExportRVA). Values range from -1 (strong negative correlation) to 1 (strong positive correlation). Notable observations include a moderate positive correlation (0.46) between DebugRVA and IntVRA, suggesting structural dependencies in executable files, and a negative correlation (-0.34) between MajorOSVersion and SizeOfStackReserve, highlighting potential OS-specific behavioral patterns. Features such as BitcoinAddresses and ResourceSize exhibit minimal correlations, underscoring their independence in the dataset. This visualization informs feature selection and model interpretability, emphasizing relationships critical to anomaly detection.

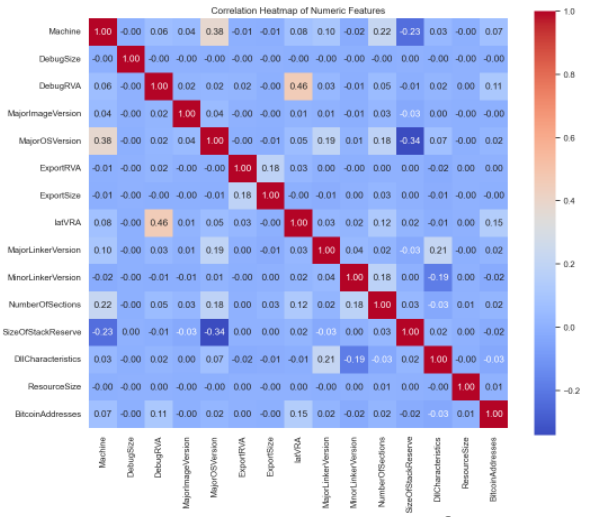

Figure 8 Correlation Heat Map of Numeric Features

Table 3 Feature Importance Analysis

Features	Random Forest	XGBoost
AS Path Length Variability	0.32	0.28
PE NumberOfSections	0.25	0.24
BGP Update Frequency	0.18	0.20
DebugRVA (PE)	0.12	0.15
BitcoinAddresses	0.05	0.04

From Table 3. The Feature importance analysis revealed AS Path Length Variability and PE NumberOfSections as dominant predictors, aligning with prior studies on BGP hijacking and malware structural analysis.

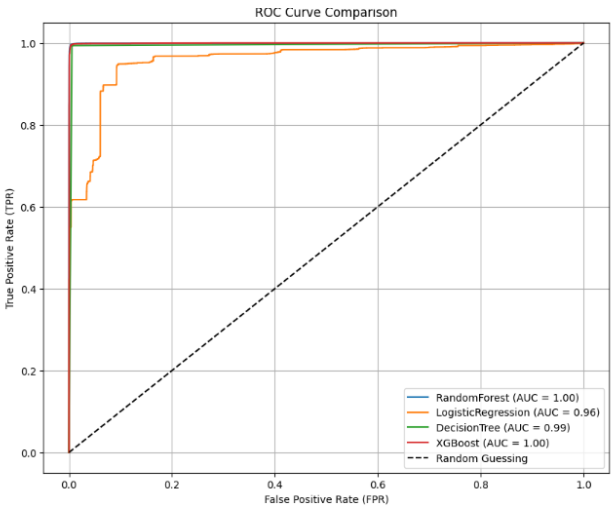

Figure 9 Receiver Operating Characteristic Curve

The plot is an ROC (Receiver Operating Characteristic) Curve in Figure 9. Comparison Figure analyzing the performance of four machine learning models: Random Forest (AUC = 1.00), Logistic Regression (AUC = 0.96), Decision Tree (AUC = 0.99), and XGBoost (AUC = 1.00). The X-axis (False Positive Rate - FPR) is the ratio of correctly classified negatives but as errors or positives, while the Y-axis (True Positive Rate - TPR) is the ratio of correctly classified positives. The diagonal dashed line is an example of random guessing (AUC = 0.5), used as a base. The curves show how the models can discriminate between classes with better performance indicated by higher AUC values. Both Random Forest and XGBoost have a perfect classification (AUC =

1.00), Decision Tree slightly lower at 0.99, and Logistic Regression, although slightly lower at 0.96, still shows good classification capability. The curves are heavily biased towards the top-left corner, showing high performance in all models. From the Figure 10. Overall, Random Forest and XGBoost exhibit the best performance, while Logistic Regression shows comparatively lower accuracy but remains effective with a high AUC.

```
=== Performance Summary ===
RandomForest:
  Accuracy = 0.9960
  AUC      = 0.9991

LogisticRegression:
  Accuracy = 0.8454
  AUC      = 0.9585

DecisionTree:
  Accuracy = 0.9937
  AUC      = 0.9939

XGBoost:
  Accuracy = 0.9951
  AUC      = 0.9996
```

Figure 10 Accuracy and AUC

This visualization drives feature selection and model interpretability, highlighting relations most important for anomaly detection. The visualization dashboard enabled forensic examination and generates a report, which helped enhance operation efficiency as shown in the Figure 11. Administrators could utilize temporal graphs and heatmaps to observe patterns and filter out anomalies based on severity (e.g., critical, high, low). The dashboard confirmed the capability of the system to detect integrated threats by identifying a simulated BGP hijacking event in just seconds and correlating it with simultaneous malicious file activity.

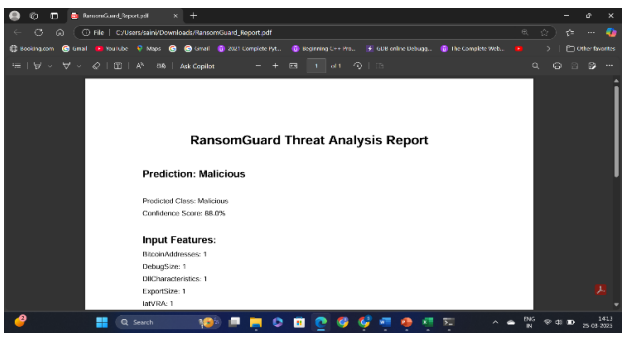

Figure 11 Analysis Report of Ransom Guard

vector anomaly detection when supervised and unsupervised machine learning models are integrated. The system is placed as a scalable solution for modern cybersecurity issues because of the high accuracy of the Random Forest classifier and the adaptability of Isolation Forest in reacting to emerging threats. The solution addresses evolving demands of global internet security by merging network and file-level analysis, enhancing detection rates and providing actionable intelligence through advanced visualization. Through the presentation of a framework for subsequent studies in adaptive, machine learning-based threat mitigation, these results contribute to the broader discourse on proactive cyber defense.

Conclusion

The system presents a hybrid machine learning mechanism that blends supervised Random Forest and unsupervised Isolation Forest models together to identify BGP and file-based abnormalities with superior accuracy and adaptability. The solution, supported by a visualization dashboard for live monitoring, connects malicious file activities with network-level issues (e.g., route hijacking). Future work will involve expanding to cloud and IoT environments, minimizing latency via edge computing, and applying deep learning (e.g., GNNs) to encrypted traffic analysis. Proactive defense can be further enhanced by predictive analytics and automated response mechanisms, and scalability would be ensured by verification across 5G/SDN architectures. The aim of these advancements is to counteract evolving cyberthreats in decentralized systems.

Acknowledgements

The authors gratefully acknowledge the referees for providing appropriate feedback and valuable remarks. The time and effort devoted to reviewing the manuscript are genuinely acknowledged.

References

[1]. P. Azugo, H. Venter, and M. W. Nkongolo, "Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset," arXiv preprint arXiv:2404.12855, Apr. 2024. [Online]. Available: https:// arxiv.org/ abs/2404.12855

[2]. S. J. Nhlapo and M. W. Nkongolo, "Zero-day attack and ransomware detection," arXiv preprint arXiv:2408.05244, Aug. 2024. [Online]. Available: https://

arxiv.org/abs/2408.05244

[3]. S. Peng et al., "MAD-MulW: A Multi-Window Anomaly Detection Framework for BGP Security Events," arXiv preprint arXiv:2312.11225, Dec. 2023. [Online]. Available: https:// arxiv.org/ abs/ 2312.11225

[4]. S. K. D. R. V. A. et al., "Enhancing Ransomware Detection in Cybersecurity: A Comprehensive Ensemble Approach," Journal of Electrical Systems, vol. 20, no. 10s, 2024. [Online]. Available: https://journal.esrgroups.org/jes/article/view/6235

[5]. J. Zhu et al., "A few-shot meta-learning based siamese neural network using entropy features for ransomware classification," arXiv preprint arXiv:2402.11342, Feb. 2024. [Online]. Available: https:// arxiv.org/ abs/ 2402.11342

[6]. S. J. Nhlapo and M. W. Nkongolo, "Zero-day attack and ransomware detection," arXiv preprint arXiv:2408.05244, Aug. 2024. [Online]. Available: https:// arxiv.org/abs/2408.05244

[7]. P. Azugo, H. Venter, and M. W. Nkongolo, "Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset," arXiv preprint arXiv:2404.12855, Apr. 2024. [Online]. Available: https:// arxiv.org /abs/2404.12855

[8]. M. L. Gonzalez et al., "Enhancing Ransomware Detection in Cybersecurity: A Comprehensive Ensemble Approach," Journal of Electrical Systems, vol. 20, no. 10s, 2024. [Online]. Available: https:// journal.esrgroups.org/jes/article/view/6235

[9]. J. Zhu et al., "A few-shot meta-learning based siamese neural network using entropy features for ransomware classification," arXiv preprint arXiv:2402.11342, Feb. 2024. [Online]. Available: https://arxiv.org/abs/2402.11342

[10]. P. Azugo, H. Venter, and M. W. Nkongolo, "Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset," arXiv preprint arXiv:2404.12855, Apr. 2024. [Online]. Available: https://arxiv.org/abs/2404.12855

[11]. S. J. Nhlapo and M. W. Nkongolo, "Zero-day attack and ransomware detection," arXiv preprint arXiv:2408.05244, Aug. 2024. [Online]. Available: https://arxiv.org/abs/2408.05244

P. Azugo, H. Venter, and M. W. Nkongolo, "Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset," arXiv preprint arXiv:2404.12855, Apr. 2024. [

[12]. S. K. D. R. V. A. et al., "Enhancing Ransomware Detection in Cybersecurity: A Comprehensive Ensemble Approach," Journal of Electrical Systems, vol. 20, no. 10s, 2024. [Online]. Available: https://journal.esrgroups.org/jes/article/view/6235

[13]. J. Zhu et al., "A few-shot meta-learning based siamese neural network using entropy features for ransomware classification," arXiv preprint arXiv:2402.11342, Feb. 2024. [Online]. Available: https://arxiv.org/abs/2402.11342

[14]. S. J. Nhlapo and M. W. Nkongolo, "Zero-day attack and ransomware detection," arXiv preprint arXiv:2408.05244, Aug. 2024. [Online]. Available: https://arxiv.org/abs/2408.05244